

#3
3-15-02

PATENT
81800.0179

Express Mail Label No. EL 713 632 464 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yoshifumi TANIMOTO

Serial No: Not assigned

Filed: January 23, 2002

For: EMAIL PROCESSING METHOD, EMAIL
PROCESSING APPARATUS AND
RECORDING MEDIUM

Art Unit: Not assigned

Examiner: Not assigned



TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

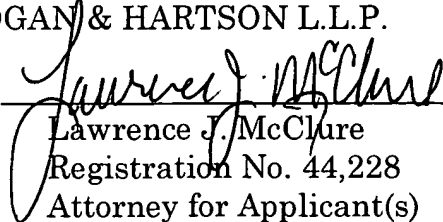
Enclosed herewith is a certified copy of Japanese patent application No. 2001-017516 which was filed January 25, 2001, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 23, 2002

By: 
Lawrence J. McClure
Registration No. 44,228
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1046 U.S. PTO
10/057685
01/23/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年 1月25日

出 願 番 号
Application Number:

特願2001-017516

出 願 人
Applicant(s):

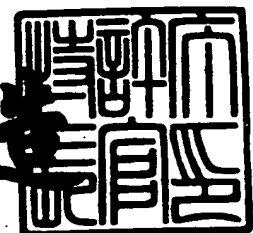
村田機械株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月24日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 21791

【提出日】 平成13年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00
G06F 19/00

【発明の名称】 電子メール処理方法及び記録媒体

【請求項の数】 4

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株式会社 本社工場内

【氏名】 谷本 好史

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06(6944)4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06(6944)4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子メール処理方法及び記録媒体

【特許請求の範囲】

【請求項 1】 一以上の宛先が登録された宛先リストに対して電子メールを送信する電子メール処理方法において、前記宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成するステップと、生成した共通鍵を用いて暗号化したデータを含む電子メールを送信するステップとを含むことを特徴とする電子メール処理方法。

【請求項 2】 一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信した場合、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成するステップと、生成した共通鍵を用いて前記暗号化データを復号するステップとを含むことを特徴とする電子メール処理方法。

【請求項 3】 コンピュータに、一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成させるプログラムコード手段と、生成させた共通鍵を用いて暗号化したデータを含む電子メールを送信させるプログラムコード手段とを含むプログラムが記録してあることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 4】 一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信したコンピュータに、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成させ、生成させた共通鍵を用いて前記暗号化データを復号させるプログラムコード手段を含むプログラムが記録してあることを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えばメーリングリストを利用することにより、同一のデータを含む電子メールを複数の電子メールアドレスに対して送信する場合、またそのようにして送信された電子メールを受信した場合の電子メール処理方法、及びその方法を実施するための装置としてコンピュータを機能させる為のコンピュータプログラムが記録されている記録媒体に関する。

【0002】

【従来の技術】

近年、コンピュータネットワークの急速な進展に伴い、安全なデータ通信を実現すべく、種々の暗号技術が注目されている。従来から、暗号化鍵及び復号鍵の両者の鍵が等しい暗号系である共通鍵暗号系、及び両者の鍵が異なる暗号系である公開鍵暗号系が広く利用されている。共通鍵暗号系の典型例としては米国商務省標準局が採用したDES (Data Encryption Standards) を、また公開鍵暗号系の典型例としてはRSA (Rivest Shamir Adleman) を夫々挙げることができる。

【0003】

一方、各ユーザの住所、氏名、電子メールアドレス等の個人を特定するID (Identity) 情報を利用する暗号系が提案されている。この暗号系では、ID情報に基づいて送受信者間で共通の暗号化鍵を生成する。

【0004】

このようなID情報に基づく暗号系であって、暗号文通信に先立って送受信者間での予備通信を必要としないものとして、ID-NIKS (ID-based non-interactive key sharing scheme) が研究され提案されている。このID-NIKSは、送受信者間で公開鍵、秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも不要であるので、任意のユーザ間で安全に通信を行うことができ、しかも、上述したように予備通信を必要としないので、ユーザの利便性が高いという利点を有している。そのため、将来の暗号系の中樞をなすものと期待されている。

【0005】

図5はID-NIKSのシステムの原理を示す説明図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共有鍵生成システムを構成している。図5において、エンティティAのID情報は、ハッシュ関数 $h(\cdot)$ を用いて $h(IDA)$ で表す。センタは、任意のエンティティAに対して、センタ公開情報 $\{PCi\}$ 、センタ秘密情報 $\{SCi\}$ 及びエンティティAのID情報 $h(IDA)$ に基づいて、以下の如く秘密鍵 SAi を計算し、エンティティAへ配布する。

$$SAi = Fi(\{SCi\}, \{PCi\}, h(IDA))$$

【0006】

エンティティAは、他の任意のエンティティBとの間に行う通信の暗号化および復号のための共通鍵 KAB を、エンティティA自身の秘密鍵 $\{SAi\}$ 、センタ公開情報 $\{PCi\}$ 及びエンティティBのID情報 $h(IDB)$ を用いて以下の如く生成する。

$$KAB = f(\{SAi\}, \{PCi\}, h(IDB))$$

また、エンティティBも同様にエンティティAとの間で用いる共有鍵 KBA を生成する。 $KAB = KBA$ の関係が常に成立するのであれば、共有鍵 KAB 、 KBA をエンティティA、B間で暗号化鍵および復号鍵として利用することができる。

【0007】

上述したID-NIKSを利用して電子メールの送受信を行う場合について説明する。まず、電子メールの送信者及び受信者は、自己の電子メールアドレス（ID情報）に基づいて定められた秘密鍵を予めセンタから夫々取得しておく。そして、送信者は、受信者の電子メールアドレス（ID情報）に基づいて生成された公開鍵と前記取得した秘密鍵とに基づいて共通鍵を生成し、生成した共通鍵を用いてデータを暗号化し、その暗号化したデータを電子メールにて送信する。一方、受信者は、送信者の電子メールアドレス（ID情報）に基づいて生成された公開鍵と前記取得した秘密鍵とに基づいて共通鍵を生成し、受信した電子メール中のデータを前記生成した共通鍵を用いて復号する。

【0008】

このようにして暗号化及び復号を行うことにより、安全な電子メールの送受信を容易に実現することができる。なお、このようなID-NIKSにおける暗号通信には、例えば上述したDES等を用いることができる。

【0009】

【発明が解決しようとする課題】

ところで、同一の電子メールを複数の宛先に対して送信する方法として、メーリングリストが広く利用されている。メーリングリストを利用する場合、メーリングリストを運営する電子メールサーバにより、そのメーリングリストに予め登録されている電子メールアドレスに対して電子メールが同報配信される。その結果、複数の利用者が同一の電子メールを受信することができる。

【0010】

しかしながら、ID-NIKSにおいては、上述したように送信者は自己の秘密鍵及び受信者の電子メールアドレスを用いてデータを暗号化する必要があるので、複数の受信者に同一の電子メールを送信するときであっても、それら受信者の電子メールアドレス夫々を用いてデータの暗号化を実行し、暗号化したデータを含む各電子メールを夫々送信しなければならず、上述したようなメーリングリストを利用することはできないという問題があった。

【0011】

本発明は斯かる事情に鑑みてなされたものであり、メーリングリスト等の一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成し、その共通鍵を用いて暗号化したデータを含む電子メールを送信し、一方この電子メールを受信した場合、宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成し、その共通鍵を用いて受信した電子メールに含まれているデータを復号することによって、宛先が複数ある場合における暗号化したデータを含む電子メールの送受信を容易に行うことができる電子メール処理方法、及びその方法を実施するための装置としてコンピュータを機能させる為のコンピュータプログラムが記録されている記録媒体を提供することを目的とする。

【 0 0 1 2 】

【課題を解決するための手段】

第1発明に係る電子メール処理方法は、一以上の宛先が登録された宛先リストに対して電子メールを送信する電子メール処理方法において、前記宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成するステップと、生成した共通鍵を用いて暗号化したデータを含む電子メールを送信するステップとを含むことを特徴とする。

【 0 0 1 3 】

第2発明に係る電子メール処理方法は、一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信した場合、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成するステップと、生成した共通鍵を用いて前記暗号化データを復号するステップとを含むことを特徴とする。

【 0 0 1 4 】

第3発明に係る記録媒体は、コンピュータに、一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された秘密鍵により共通鍵を生成させるプログラムコード手段と、生成させた共通鍵を用いて暗号化したデータを含む電子メールを送信させるプログラムコード手段とを含むプログラムが記録してあることを特徴とする。

【 0 0 1 5 】

第4発明に係る記録媒体は、一以上の宛先が登録された宛先リストに対して送信された暗号化データを含む電子メールを受信したコンピュータに、前記宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成させ、生成させた共通鍵を用いて前記暗号化データを復号させるプログラムコード手段を含むプログラムが記録してあることを特徴とする。

【0016】

第1発明及び第3発明による場合、例えばメーリングリスト等のように、一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵と、電子メールを送信する送信元の電子メールアドレスに基づいて生成された秘密鍵とを用いて共通鍵を生成し、その生成した共通鍵を用いて送信対象であるデータを暗号化した後にその暗号化したデータを含む電子メールを送信する。

【0017】

これにより、複数の電子メールアドレスに対して電子メールを送信する場合であっても、それらの電子メールアドレス夫々に基づいて暗号化したデータを含む各電子メールを夫々送信する必要はなく、それらの電子メールアドレスが登録されている宛先リストの電子メールアドレスを用いて暗号化を実行し、その結果暗号化されたデータを含む一の電子メールを送信するだけで足りる。よって、暗号化されたデータを含む電子メールを複数の宛先に対して容易に送信することができる。

【0018】

第2発明及び第4発明による場合、一以上の宛先が登録された宛先リスト宛に送信された暗号化データを含む電子メールを受信した場合、宛先リストの電子メールアドレスに基づいて生成された秘密鍵と、電子メールを送信した送信元の電子メールアドレスに基づいて生成された公開鍵とを用いて共通鍵を生成し、その生成した共通鍵を用いて受信した電子メールに含まれている暗号化データを復号する。

【0019】

これにより、一以上の宛先が登録された宛先リスト及び電子メールの送信元夫々の電子メールアドレスを用いて生成された共通鍵により暗号化されたデータを容易に復号し、内容を確認することができる。

【0020】

【発明の実施の形態】

以下、本発明をその実施の形態を示す図面に基づいて詳述する。

図1は、本発明の電子メール処理方法を実施するための装置として機能するパ

ーソナルコンピュータPC1,PC2,...,PCn (nは自然数)と、これらのパーソナルコンピュータPC1,PC2,...,PCnが接続されているコンピュータネットワークとの構成例を示すブロック図である。

【 0 0 2 1 】

図1において、NTW はコンピュータネットワークであるインターネットを示しており、このインターネットNTW には、インターネットNTW への接続業者である多数のプロバイダPR1,PR2,...,PRn (nは自然数)が接続されている。

【 0 0 2 2 】

プロバイダPR1,PR2,...,PRnは、これらと契約したクライアントに対して電子メールの送受信サービスを提供する電子メールサーバとして機能するサーバSV1,SV2,...,SVn (nは自然数)を夫々備えている。

【 0 0 2 3 】

またプロバイダPR1,PR2,...,PRnのサーバSV1,SV2,...,SVnには、ルータRT1,RT2,...,RTn (nは自然数)及びアナログ回線Lを介してクライアントとしてのパーソナルコンピュータPC1,PC2,...,PCnが夫々接続されている。なお、ルータRT1,RT2,...,RTnに代えて、公衆電話回線の交換機を用いてもよい。

【 0 0 2 4 】

センタCは、秘密鍵として機能する第1秘密鍵PRK1-1,PRK1-2,...,PRK1-nを各ユーザに対して夫々発行する。これらの第1秘密鍵PRK1-1,PRK1-2,...,PRK1-nは、各ユーザが利用する電子メールアドレスに基づいて夫々定められており、電子メール等の手段を用いて各パーソナルコンピュータPC1,PC2,...,PCnへ夫々送信される。

【 0 0 2 5 】

またセンタCは、同じく秘密鍵として機能する第2秘密鍵PRK2をメーリングリストに対して発行する。この第2秘密鍵PRK2は、メーリングリストの電子メールアドレスに基づいて定められており、電子メール等の手段を用いて、そのメーリングリストを運営する電子メールサーバ(以下、MLサーバという)MSへ送信される。

【 0 0 2 6 】

MLサーバMSは、上述したようにしてセンタCから受信した第2秘密鍵PRK2を含む電子メールを、メーリングリストに登録されている電子メールアドレス宛に送信する。これにより、各パーソナルコンピュータPC1, PC2, ..., PCnは第2秘密鍵PRK2を取得することができる。

【0027】

なお、各パーソナルコンピュータPC1, PC2, ..., PCnがセンタCから第1秘密鍵PRK1を又はMLサーバMSから第2秘密鍵PRK2を夫々取得する方法、またMLサーバSV3がセンタCから第2秘密鍵PRK2を取得する方法としては、上述した電子メールを利用する以外にも、例えばそれらの秘密鍵を記憶させたフレキシブルディスクを郵送等の手段により受け取ることによって取得するようにしてもよい。

【0028】

さらに、ネットワークNTWには、データベースサーバDSが接続されている。このデータベースサーバDSは、本発明に係る電子メール送信装置のプログラムを記録している記録媒体DBを備えている。

【0029】

図2は、本発明の電子メール処理方法を実施するための装置として機能するパーソナルコンピュータPC1の構成を示すブロック図である。なお、パーソナルコンピュータPC2, ..., PCnの構成は、パーソナルコンピュータPC1の場合と同様であるので説明を省略する。

図2において、1はCPU及びキャッシュメモリ等で構成される制御部であり、該制御部1は、バス8を介して接続された各ハードウェア各部を制御すると共に、後述するハードディスク4に記憶されている種々のコンピュータプログラムを実行する。

【0030】

RAM2は、SRAM又はDRAM等で構成され、制御部1において発生した一時的なデータを記憶する。

【0031】

外部記憶装置3は、CD-ROMドライブ又はフレキシブルディスクドライブ等で構成され、本発明の電子メール送信方法及び電子メール処理方法に係るプロ

グラムが記録されているCD-ROM又はフレキシブルディスク等の可搬型記録媒体10から前記プログラムを読み取る。

【0032】

ハードディスク4は、読み書き可能な磁気ディスクから構成され、外部記憶装置3により読み取った本発明の電子メール装置のプログラム、及びパーソナルコンピュータPC1の動作に必要な種々のコンピュータプログラムを記憶する。

【0033】

また、このハードディスク4は、上述したようにしてセンタCから取得した第1秘密鍵PRK1-1及び第2秘密鍵PRK2を記憶している。

【0034】

なお、図2はパーソナルコンピュータPC1の構成を示しているため、ハードディスク4は第1秘密鍵PRK1-1を記憶しているが、パーソナルコンピュータPC2, ..., PCnの場合、ハードディスク4は第1秘密鍵PRK1-2, ..., PRK1-nを夫々記憶している。

【0035】

また、後述するように、第1秘密鍵PRK1-1は電子メールを送信する場合に用いられ、また第2秘密鍵PRK2はメーリングリストに係る電子メールを受信する場合に用いられる。したがって、パーソナルコンピュータPC1が電子メールを送信するのみであって、メーリングリストに係る電子メールを受信することがない場合は、第2秘密鍵PRK2がハードディスク4に記憶されていなくてもよい。

【0036】

モデム5は、インターネットNTWを介してデータ通信を行うための通信インタフェースであり、アナログ回線Lとの閉結及び解放の動作を行う。なお、モデム5の代わりに、DSU (Digital Service Unit) を用いることにより、ベースバンド伝送方式のデジタル回線と接続するようにしてもよい。

【0037】

表示部6は、CRTディスプレイ又は液晶表示装置(LCD)等の表示装置であり、パーソナルコンピュータPC1の動作状態を表示したり、種々の入出力データの表示を行う。また、操作部7は、パーソナルコンピュータPC1を操作するた

めに必要なキーボード等の入力装置である。

【0038】

なお、本発明の電子メール処理方法に係るプログラムは、上述したようにして可搬型記録媒体10から読み取る以外にも、インターネットNTWを介して上述したデータベースサーバDSに接続し、このデータベースサーバDSが備えている記録媒体DBからパーソナルコンピュータPC1へ前記プログラムをダウンロードすることができる。そして、そのダウンロードしたプログラムをハードディスク4に記憶し、記憶したプログラムを制御部1がRAM2にロードすることによって、パーソナルコンピュータPC1は後述する処理を実行することができる。

【0039】

次に、パーソナルコンピュータPC1, PC2, ..., PCnの動作について説明する。

図3は、パーソナルコンピュータPC1がメーリングリスト宛に電子メールを送信する場合の制御部1の処理手順を示すフローチャートである。なお、パーソナルコンピュータPC1は、接続契約をしているプロバイダPR1に対してユーザID、パスワード等を送出することによりログインしているものとする。

【0040】

MLサーバMSが運営しているメーリングリストに参加しているユーザは、操作部7を操作することにより、電子メールの宛先である前記メーリングリストの電子メールアドレスを入力し、また電子メールにて送信するデータを入力する。そして、ユーザは、その電子メールの送信をパーソナルコンピュータPC1に対して指示する。

【0041】

パーソナルコンピュータPC1が備える制御部1は、電子メールの送信指示をユーザから受け付けた場合、上述したようにして入力されたメーリングリストの電子メールアドレスに基づいて定められた公開鍵及びハードディスク4に記憶されている第1秘密鍵PRK1-1を読み込む(S11)。

【0042】

次に、ステップS11にて読み込んだ公開鍵及び第1秘密鍵PRK1-1を用いて共通鍵を生成する(S12)。そして、このようにして生成した共通鍵を用いて、

上述したようにして入力された送信対象のデータを暗号化する（S 1 3）。

【 0 0 4 3 】

次に、上述したようにして入力されたメーリングリストの電子メールアドレスを宛先に設定し、ステップ S 1 3 にて暗号化したデータを用いて電子メールを作成し（S 1 4）、作成した電子メールを送信する（S 1 5）。

【 0 0 4 4 】

このようにしてパーソナルコンピュータ PC1 から送信された電子メールは、サーバ SV1 を介して MLサーバ MS によって受信される。そして、MLサーバ MS は、パーソナルコンピュータ PC1 から受信した電子メールをメーリングリストに登録されている電子メールアドレス宛に同報送信する。

【 0 0 4 5 】

図 4 は、パーソナルコンピュータ PC2, …, PCn がメーリングリストに係る電子メールを受信した場合の制御部 1 の処理手順を示すフローチャートである。なお、パーソナルコンピュータ PC2, …, PCn は、接続契約をしているプロバイダ PR2, …, PRn に対してユーザ ID、パスワード等を送出することにより夫々ログインしているものとする。

【 0 0 4 6 】

MLサーバ MS が運営しているメーリングリストに参加している各ユーザは、パーソナルコンピュータ PC2, …, PCn に対して電子メールを受信するように指示する。パーソナルコンピュータ PC2, …, PCn が備える制御部 1 は、電子メールの受信指示をユーザから受け付けた場合、上述したようにして MLサーバ MS から送信されたメーリングリストに係る電子メールをサーバ SV2, …, SVn から受信し、その受信した電子メールを読み込む（S 2 1）。

【 0 0 4 7 】

次に、ハードディスク 4 に記憶されている第 2 秘密鍵 PRK2 を読み込む（S 2 2）。そして、その読み込んだ第 2 秘密鍵 PRK2 とステップ S 2 1 にて読み込んだ電子メールの送信者の電子メールアドレスに基づいて生成された公開鍵とを用いて、共通鍵を生成し（S 2 3）、生成した共通鍵を用いて前記受信した電子メールのデータを復号する（S 2 4）。

【0048】

これにより各ユーザはメーリングリストに係る暗号化された電子メールの内容を確認することができる。

【0049】

なお、本実施の形態ではメーリングリストを利用して電子メールの送受信を行っているが、メーリングリスト以外であっても、一の電子メールアドレスを宛先とした場合に複数の宛先に対して同一の電子メールを同報送信することができる仕組みであれば、本発明を適用することが可能である。

【0050】

【発明の効果】

以上詳述した如く、本発明によれば、メーリングリスト等の一以上の宛先が登録された宛先リストの電子メールアドレスに基づいて生成された公開鍵及び送信元の電子メールアドレスに基づいて生成された共通鍵により共通鍵を生成し、その共通鍵を用いて暗号化したデータを含む電子メールを送信し、一方この電子メールを受信した場合、宛先リストの電子メールアドレスに基づいて生成された秘密鍵及び送信元の電子メールアドレスに基づいて生成された公開鍵により共通鍵を生成し、その共通鍵を用いて受信した電子メールに含まれているデータを復号することによって、宛先が複数ある場合における暗号化したデータを含む電子メールの送受信を容易に行うことができる等、本発明は優れた効果を奏する。

【図面の簡単な説明】

【図1】

本発明の電子メール処理方法を実施するための装置として機能するパーソナルコンピュータと、これらのパーソナルコンピュータが接続されているコンピュータネットワークとの構成例を示すブロック図である。

【図2】

パーソナルコンピュータの構成を示すブロック図である。

【図3】

パーソナルコンピュータがメーリングリスト宛に電子メールを送信する場合の制御部の処理手順を示すフローチャートである。

【図 4】

パーソナルコンピュータがメーリングリストに係る電子メールを受信した場合の制御部の処理手順を示すフローチャートである。

【図 5】

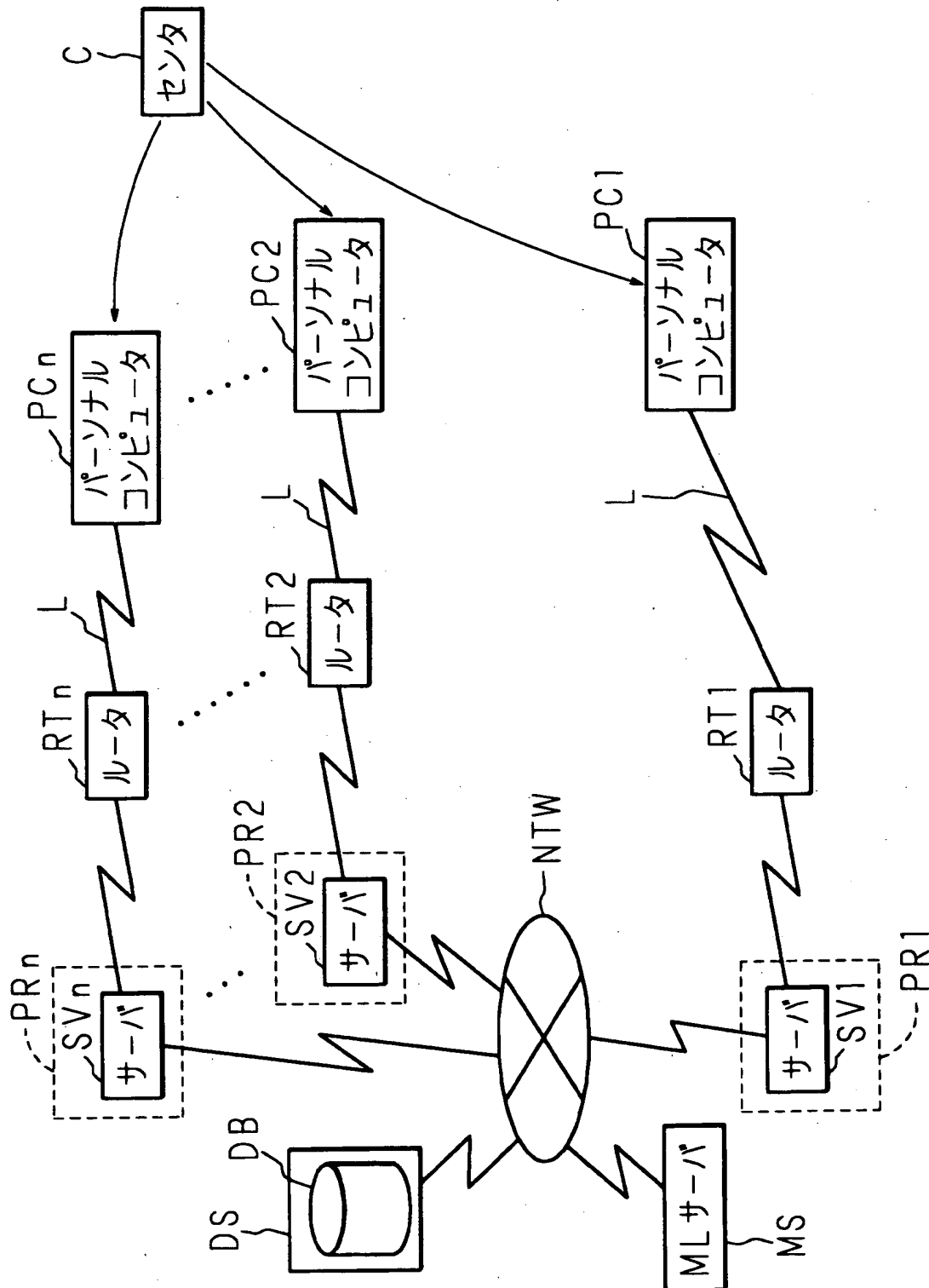
ID-NIKSのシステムの原理を示す説明図である。

【符号の説明】

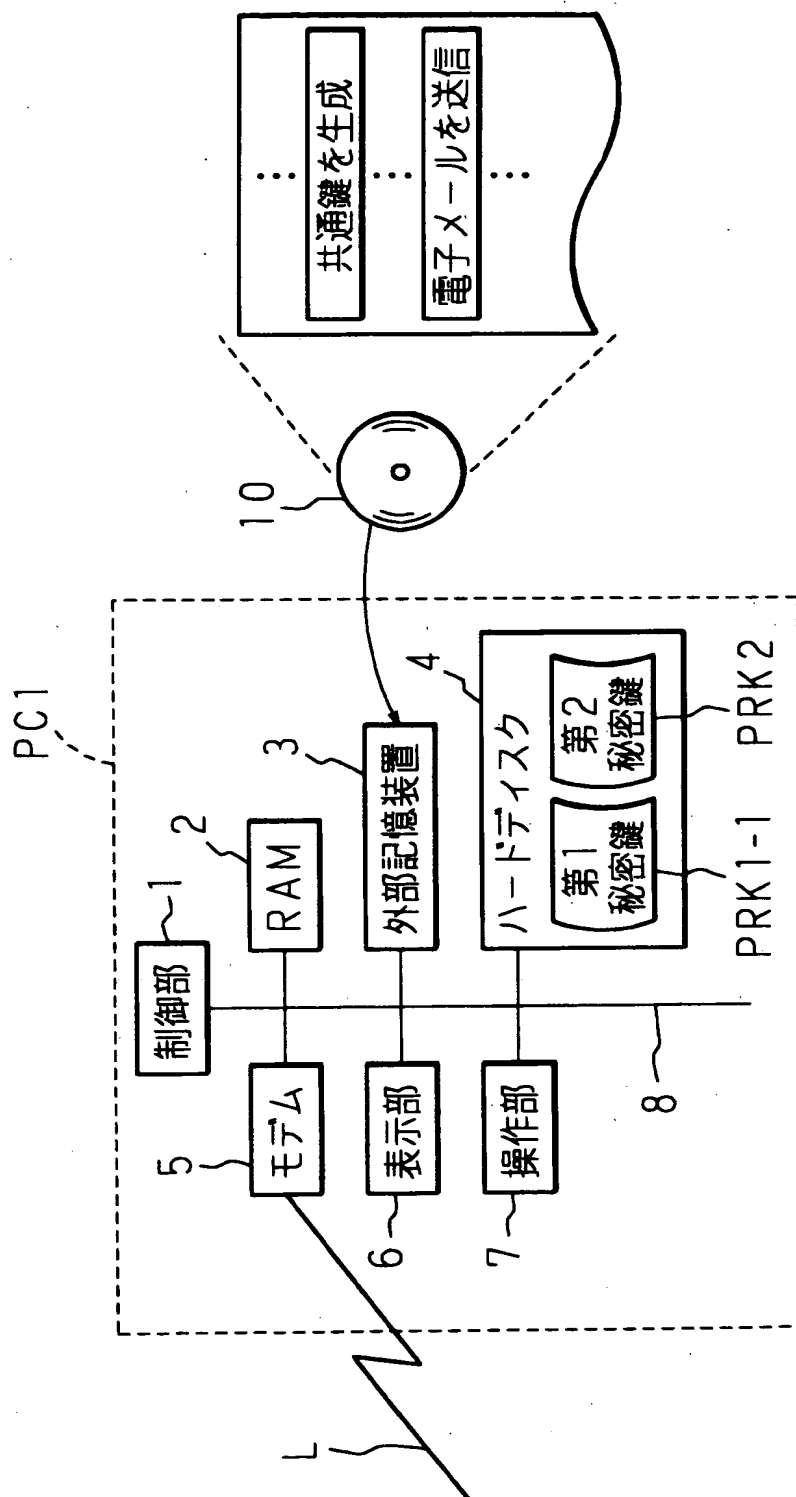
- 1 制御部
- 2 RAM
- 3 外部記憶装置
- 4 ハードディスク
- 5 モデム
- 6 表示部
- 7 操作部
- C センタ
- MS メーリングリストサーバ
- NTW インターネット
- PC1, PC2, ..., PCn パーソナルコンピュータ
- PRK1-1 第1秘密鍵
- PRK2 第2秘密鍵

【書類名】 図面

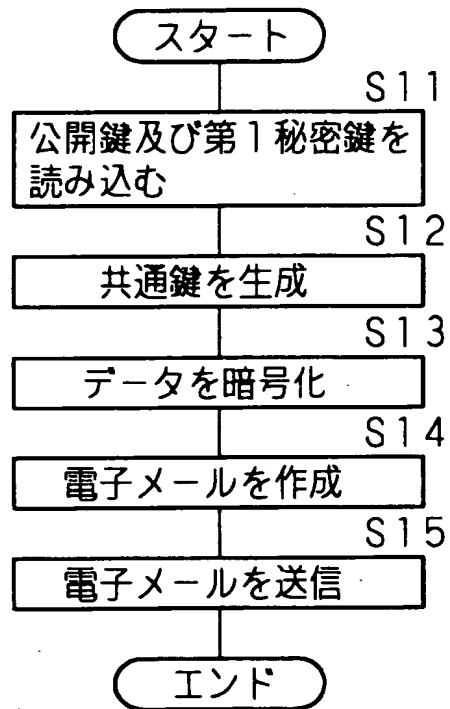
【図1】



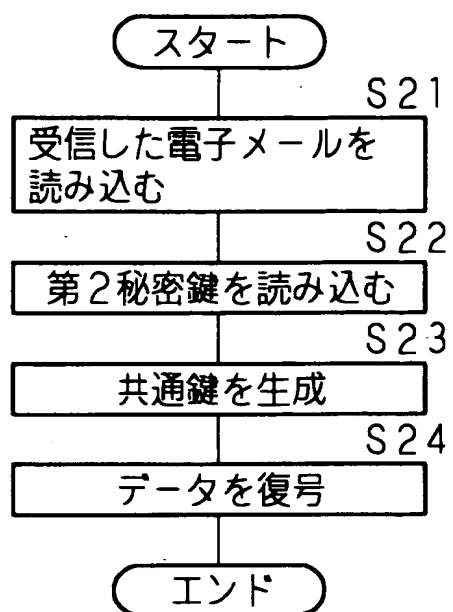
【図2】



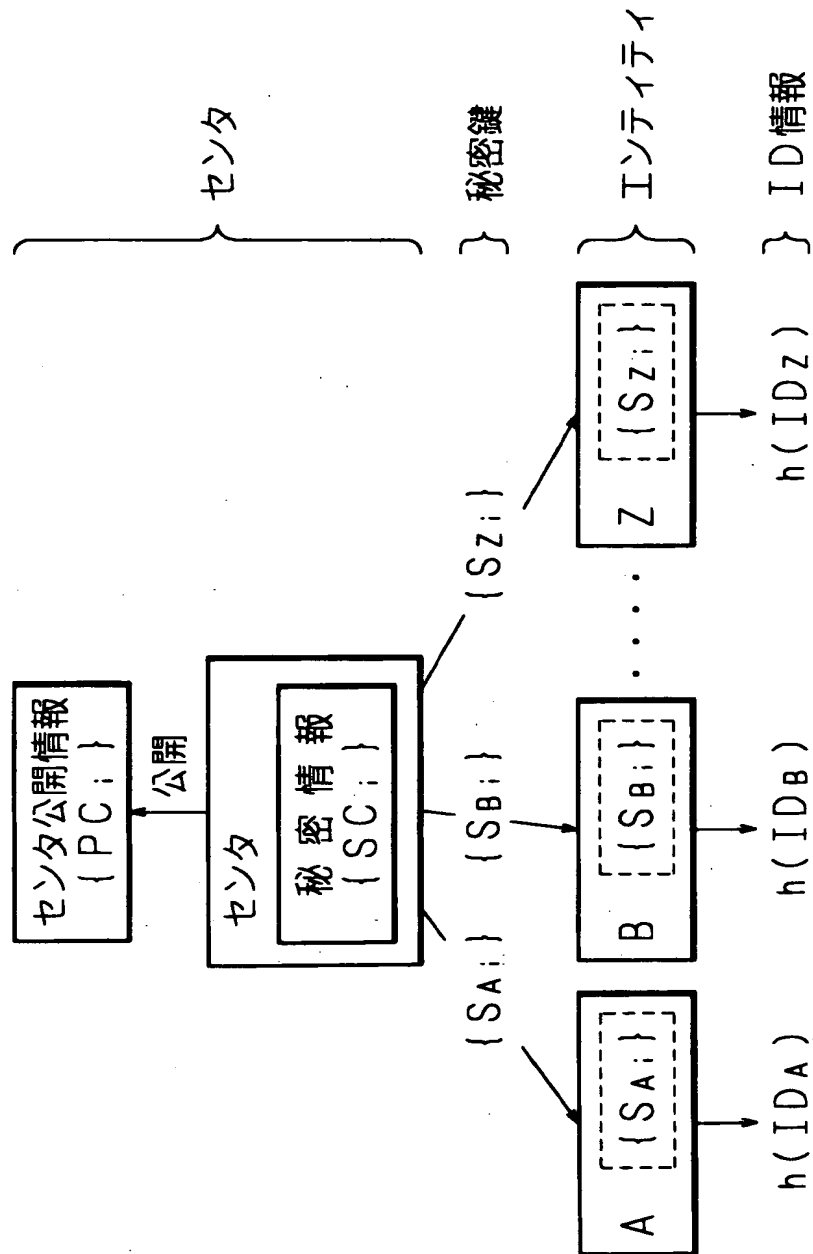
【図3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 暗号化されたデータを含む電子メールを効率的に同報送信することができる電子メール処理方法及び記録媒体の提供。

【解決手段】 パーソナルコンピュータPC1 は、メーリングリストを宛先とした電子メールの送信指示をユーザから受け付けた場合、そのメーリングリストの電子メールアドレスに基づいて生成された公開鍵及び予めセンタから取得した秘密鍵を用いて共通鍵を生成し（S 1 2）、生成した共通鍵を用いて送信対象のデータを暗号化する（S 1 3）。そして、その暗号化したデータを含む電子メールをメーリングリスト宛に送信する（S 1 5）。

【選択図】 図 3

出 願 人 履 歷 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地

氏 名 村田機械株式会社